(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－290418
（P2002－290418A）
(43)公開日　平成14年10月４日(2002.10.4)

| (51)Int.Cl.' | | 識別記号 | FI | | テーマコード'(参考) |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 12/28 | ３００ | Ｈ０４Ｌ | 12/28 | ３００Ｚ　５Ｊ１０４ |
| | | １００ | | | １００Ｈ　５Ｋ０３２ |
| Ｈ０４Ｂ | 3/54 | | Ｈ０４Ｂ | 3/54 | ５Ｋ０３３ |
| Ｈ０４Ｌ | 9/08 | | Ｈ０４Ｌ | 12/40 | Ｚ　５Ｋ０４６ |
| | 9/18 | | | 9/00 | ６０１Ｃ |

審査請求　有　請求項の数10　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2001－90070(P2001－90070)

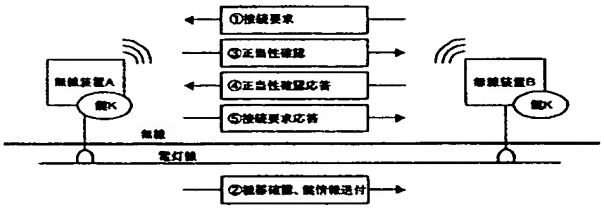
(22)出願日　平成13年３月27日(2001.3.27)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　大喜多　秀紀
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(72)発明者　山田寺　真司
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(74)代理人　100083161
弁理士　外川　英明

最終頁に続く

(54)【発明の名称】　無線装置

(57)【要約】
【課題】従来の無線装置による接続では、高セキュリティやプラグアンドプレイ接続機能を必要とする無線１３９４によるデジタル映像コンテンツの伝送には適用できない。
【解決手段】無線装置Ｂから無線装置Ａに対し接続要求を送信する。次に無線装置Ａから無線装置Ｂに対して電灯線（有線）経由で鍵情報（鍵Ｋ）を送付する。無線装置Ａは接続要求装置の正当性を確認する。無線装置Ｂは正当性確認に応答する。正当性を確認した無線装置Ａは接続要求が受理されたことを無線装置Ｂに通知し、これによりデータ通信が行われる。



1

【特許請求の範囲】

【請求項１】　無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、

前記無線通信手段で他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置と通信可能か否かに応じて無線通信するか否かをを決定することを特徴とする無線装置。

【請求項２】　無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、

前記無線通信手段により他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置の存在を、前記有線通信手段を用いて確認する手段と、

前記有線通信手段により前記他の無線装置の存在が確認できたとき、装置を識別するための情報である装置識別情報を前記有線通信手段により前記他の無線装置に送信する手段と、

前記他の無線装置が前記装置識別情報を保有しているか否かを前記無線通信手段を用いて確認する確認手段と、

前記確認手段による確認の結果、前記他の無線装置が前記装置識別情報を保有していることが確認できたとき前記他の無線装置と無線によるデータ通信を許可し、確認できないとき前記他の無線装置と無線によるデータ通信を許可しない制御手段を備えたことを特徴とする無線装置。

【請求項３】　無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、

前記無線通信手段で他の無線装置と無線通信する前に、前記有線通信手段を介した前記他の無線装置の存在確認要求に応答する存在確認応答手段と、

前記無線通信手段で前記他の無線装置と無線通信する前に、前記他の無線装置から装置を識別するための情報である装置識別情報を、前記有線通信手段を介して受信する装置識別情報受信手段と、

前記他の無線装置からの前記無線通信手段を介した前記装置識別情報の保有確認に応答する装置識別情報応答手段と、

前記他の無線装置による無線によるデータ通信を許可するか否かの判断結果に応じて前記他の無線装置と無線によるデータ通信を行う制御手段とを備えたことを特徴とする無線装置。

【請求項４】　無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、

前記無線通信手段により他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置にスクランブル鍵情報を送信するスクランブル

2

鍵情報送信手段と、

前記無線通信手段により前記他の無線装置と無線によるデータ通信をする前に、前記無線通信手段を介して前記他の無線装置に所定のデータを送信する所定データ送信手段と、

前記他の無線装置から送られてきた、前記所定のデータを前記スクランブル鍵情報により暗号化した暗号化データを受信する暗号化データ受信手段と、

前記暗号化データを前記送信したスクランブル鍵情報に応じたデスクランブル鍵情報により復号化する復号化手段と、

前記他の無線装置に送信した前記所定のデータおよび前記復号化手段により復号化されたデータが同じか否かを判定する判定手段と、

前記判定手段の判定結果が同じと判定されたときに前記無線通信手段を介して前記他の無線装置と無線によるデータ通信を許可し、同じでないと判定したときに前記無線通信手段を介して前記他の無線装置との無線によるデータ通信を許可しない制御手段とを備えたことを特徴とする無線装置。

【請求項５】　無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、

前記無線通信手段で他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置からスクランブル鍵情報を受信するスクランブル鍵情報受信手段と、

前記無線通信手段で前記他の無線装置と無線によるデータ通信をする前に、前記無線通信手段を介して入力された所定のデータを受信する所定データ受信手段と、

前記所定のデータを前記スクランブル鍵情報により暗号化した暗号化データを、前記他の無線装置へ送信する暗号化データ送信手段と、

前記他の無線装置が前記暗号化データを受信し判定した結果に応じて、前記無線通信手段を介して前記他の無線装置と無線によるデータ通信を制御する制御手段とを備えたことを特徴とする無線装置。

【請求項６】　前記スクランブル鍵情報を記憶する記憶手段を有し、

前記暗号化データ送信手段は、前記有線通信手段が有線接続されていない状態でも、前記無線通信手段を介して入力された前記所定のデータを前記記憶手段に記憶されている前記スクランブル鍵情報により暗号化した暗号化データを前記他の無線装置へ送信することを特徴とする請求項５に記載の無線装置。

【請求項７】　前記装置識別情報は、データ暗号化のための鍵情報であることを特徴とする請求項２または３に記載の無線装置。

【請求項８】　前記装置識別情報は、無線通信のための設定情報であることを特徴とする請求項２または３に記

載の無線装置。

【請求項９】　前記有線通信手段は、電灯線または有線のＩＥＥＥ１３９４ネットワークであることを特徴とする請求項２、３、５、６のいずれか１項に記載の無線装置。

【請求項１０】　前記有線通信手段は電灯線に接続されており、この電灯線は家庭内の別の電灯線に情報を転送するブレーカ装置を含むことを特徴とする請求項２、３、５、６のいずれか１項に記載の無線装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ネットワーク接続される装置に関し、特に無線によりネットワークに接続される装置に関する。

【０００２】

【従来の技術】従来、無線装置において無線経由でアクセス要求があった場合、家庭内の装置と隣接する家に設置されている外部の装置とを区別する手段が無いため、外部から不正にアクセスされる問題がある。これに対し装置毎に暗証番号等の装置識別情報を人手で設定し区別する手段が考えられるが、装置台数が多い場合や装置操作に不慣れな利用者には適用しにくいという問題があった。

【０００３】これら暗証番号を用いた無線装置については、例えば特開平１１－１４６４５２号公報に開示されている。この公報に開示されている技術では、登録子機にそれぞれ暗証番号を設定しておき、該登録子機からＩＤ情報を取得することで外部からの不正な登録でないかを区別し、新規登録子機の設定を簡便に行うものである。詳細には、子機側からモード設定可能な子機登録方式を得るため子機間通信モードにする。暗証番号と電話番号を利用し、子機２，３を通信状態とする。新規登録子機３は既登録子機２に格納されている親機のＩＤ情報のコピー要求すると、既登録子機２は親機１のＩＤ情報を送出する。新規登録子機３は既登録子機２からの親機ＩＤ情報を記憶する。子機３が親機の電波到達範囲内に来たとき親機ＩＤ情報を受信し、子機２からコピーしたＩＤ情報と比較して一致した場合には子機登録の要求を行う。親機は子機３との子機登録動作を自動的に開始し、子機登録を行う。

【０００４】しかし、この従来技術では、親機および全ての子機に対し１度は暗証番号を設定しなければならず、装置台数が多い場合作業が大変になる。更に暗証番号は人手で入力する必要があるため、映像コンテンツの伝送等コピー制御を含む高セキュリティを要求される分野には適用しにくい。例えば従来の装置における暗証番号等装置識別用のＩＤは４桁の数字等人が入力可能な短いものが一般的であり、セキュリティレベルが低く、高いセキュリティレベルを要求されるデータの伝送には不向きであった。例えばＤＶＨＳやＤＶＤやデジタル放送



等のデジタル映像コンテンツでは、コンテンツの著作権保護（不正コピー防止）が必要不可欠であり、高いセキュリティレベルが必要である。

【０００５】家庭用ＡＶ装置でのデジタル映像コンテンツの伝送に用いられるＩＥＥＥ１３９４では、ＤＴＣＰ（Digita Transmisson Content Protection）というコピー保護手段をこのコンテンツ保護のために用いる。これは各装置が公的な認証機関が発行する鍵を用いた認証により、正しく認証機関からライセンスを受けた装置同士でデジタル映像コンテンツの伝送を行う手段である。このため不正ライセンス装置にデジタル映像コンテンツが不正に流出することを防いでいる。設定なしに接続しただけで動作するプラグアンドプレイ機能を持つＩＥＥＥ１３９４では、ライセンス装置同士であれば、デジタル映像コンテンツの伝送が可能である。有線のＩＥＥＥ１３９４では、接続は家庭内の装置としか接続されていないことが容易にわかるので、プラグアンドプレイによる接続で何ら問題は生じない。

【０００６】しかしながらプラグアンドプレイ（設定なしにつなぐだけで動作する）による接続を前提としたＩＥＥＥ１３９４を無線に拡張した無線１３９４（Wireless1394）では、接続のための設定を省く必要があるため上記公報に記載された技術は適用することができず、家庭内の装置へ隣の家等から無線でプラグアンドプレイ接続することができてしまうという問題がある。

【０００７】

【発明が解決しようとする課題】このように従来の無線装置による接続では、従来簡単な暗証番号を個々の装置に設定することで装置登録を行っており、高セキュリティやプラグアンドプレイ接続機能を必要とする無線１３９４によるデジタル映像コンテンツの伝送には適用できないという問題があった。

【０００８】この発明は、特にプラグアンドプレイを前提とする無線装置間の接続時において、人手による設定を行わずに隣接した家等外部からの不正な接続要求を排除し、同一家庭内の装置のみの安全な無線通信ネットワークを構築することを目的とする。

【０００９】また、この発明は冗長な設定なしに同一家庭内装置のみが知り得る暗号鍵を用いて、データを暗号化通信し、外部からのデータ盗聴を防ぐことを目的とする。

【００１０】

【課題を解決するための手段】上記の目的を達成するために、この発明においては、無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段で他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置と通信可能か否かに応じて無線通信するか否かをを決定することを特徴とする無線装置を提供する。

5

【００１１】また、無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段により他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置の存在を、前記有線通信手段を用いて確認する手段と、前記有線通信手段により前記他の無線装置の存在が確認できたとき、装置を識別するための情報である装置識別情報を前記有線通信手段により前記他の無線装置に送信する手段と、前記他の無線装置が前記装置識別情報を保有しているか否かを前記無線通信手段を用いて確認する確認手段と、前記確認手段による確認の結果、前記他の無線装置が前記装置識別情報を保有していることが確認できたとき前記他の無線装置と無線によるデータ通信を許可し、確認できないとき前記他の無線装置と無線によるデータ通信を許可しない制御手段を備えたことを特徴とする無線装置を提供する。

【００１２】また、無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段で他の無線装置と無線通信する前に、前記有線通信手段を介した前記他の無線装置の存在確認要求に応答する存在確認応答手段と、前記無線通信手段で前記他の無線装置と無線通信する前に、前記他の無線装置から装置を識別するための情報である装置識別情報を、前記有線通信手段を介して受信する装置識別情報受信手段と、前記他の無線装置からの前記無線通信手段を介した前記装置識別情報の保有確認に応答する装置識別情報応答手段と、前記他の無線装置による無線によるデータ通信を許可するか否かの判断結果に応じて前記他の無線装置と無線によるデータ通信を行う制御手段とを備えたことを特徴とする無線装置を提供する。

【００１３】

【発明の実施の形態】（接続要求に応答する無線装置の構成）以下、本発明の実施の形態を図面を用いて詳細に説明する。

【００１４】図１は、本発明に係る接続要求に応答する無線装置の構成を説明するためのブロック図である。

【００１５】この無線装置は他の無線装置からの接続要求に対して、家庭内の無線装置からの接続であるかを確認し、安全に接続を確立する接続要求応答装置に関するものである。

【００１６】まず、無線装置１００の構成について説明する。

【００１７】図１に示すように、無線装置１００は、他の機器と無線により通信を行う無線通信部１０１、他の無線装置からの接続要求に応答する接続要求応答部１０２、他の無線装置が家庭内に存在するか否かを確認する無線装置存在確認部１０３、無線通信部１０１を介して他の無線装置の正当性を確認する正当性確認部１０４、スクランブルに用いる鍵情報を管理する鍵情報管理部１０５、無線通信部１０１とは別の系（例えば有線）で通

6

信を行う第２通信部１０６、通信するデータを暗号化・復号化する暗号化・復号化部１０７、通信するデータを送受処理するデータ処理部１０８から構成されている。

【００１８】次に、このように構成された無線装置１００の動作について詳細に説明する。

【００１９】無線通信部１０１は、他の無線装置から受信した接続要求を接続要求応答部１０２に出力する。

【００２０】接続要求応答部１０２は、無線通信部１０１から接続要求が入力されると、通信に用いるＩＤ情報を無線装置存在確認部１０３に出力する。この通信に用いるＩＤ情報の具体例としては装置固有のＭＡＣアドレスや、ＩＥＥＥ１３９４で用いられるノードＩＤ、エコーネット規格で定義されるエコーネットアドレス等がある。なお通信に用いるＩＤ情報は本発明の示す鍵情報等の装置識別情報とは別のものである。

【００２１】通信に用いるＩＤ情報はプラグアンドプレイ接続により設定なしに装置間で通信を行うために伝送されるものであるが、このＩＤ情報だけでは家庭内の装置であるか外部からのアクセスであるかを区別することはできない。家庭内装置からのアクセスを外部からの不正アクセスから区別するためには通信に用いるＩＤ情報とは別の装置識別情報が必要となる。

【００２２】無線装置存在確認部１０３は、接続要求応答部１０２から入力された通信に用いるＩＤ情報を基に、第２通信部１０６を通じて、前記接続要求を出した他の無線装置の存在を確認する。

【００２３】第２通信部１０６の具体例としては、エコーネット等で通信に用いる電灯線やＩＥＥＥ１３９４の無線拡張である無線１３９４がある。

【００２４】無線装置存在確認部１０３は、第２通信部１０６が前記接続要求を出した他の無線装置の存在を確認できた場合、この確認結果を鍵情報管理部１０５に出力する。

【００２５】鍵情報管理部１０５は、管理していた鍵情報を正当性確認部１０４へ出力すると共に、管理していた鍵情報を第２通信部１０６を経由して上記存在を確認した無線装置に出力する。本実施の形態では装置識別情報として鍵情報を用いた例を示している。鍵情報の具体例としては無線ＬＡＮで用いられるＷＥＰ鍵情報等がある。ＷＥＰ鍵情報は１２８ｂｉｔの長さをもつ鍵情報である。また装置識別情報として無線接続のための設定情報を用いることもできる。

【００２６】無線接続のための設定情報の具体例としてはチャンネルやＥＳＳ－ＩＤ等がある。無線接続手段としてＩＥＥＥ８０２．１１ｂやＩＥＥＥ８０２．１１ａで規定される無線ＬＡＮを用いる場合、個々の装置毎にチャンネルやＥＳＳ－ＩＤを設定する必要がある。この場合、接続要求装置は第２通信部１０６を経由して接続要求を行い、設定情報を接続要求装置から取得することで、第２通信部１０６により接続するだけで無線通信を

開始することが出来るようになる。なお無線通信の具体例としては他に無線１３９４やＢＬＵＥＴＯＯＴＨがある。無線通信の手段毎に接続方法や初期設定の有無等は異なり、無線接続の方法は本実施例の限りではない。

【００２７】正当性確認部１０４は正しい無線装置（家庭内の無線装置）に鍵情報が通知されたかを無線通信部１０１を経由して確認する。正当性確認の具体的な方法としては公開鍵暗号方式として一般に知られている２パス相手認証やメッセージ認証等の手法が利用できる。

【００２８】接続要求した他の無線装置が正しい無線装置（家庭内の無線装置）の場合、正当性確認部１０４は、無線通信部１０１を経由して前記接続要求を出した他の無線装置の正当性を確認した（家庭内の無線装置であることが確認できた）ことを接続要求応答部１０２へ出力する。すると接続要求応答部１０２は、接続要求を受理したことを示す接続要求受理信号を無線通信部１０１を介して他の無線装置へ出力すると共に、無線装置存在確認部１０３を介して鍵情報管理部１０５へも出力する。

【００２９】反対に、接続要求した他の無線装置が正しくない無線装置（家庭内の無線装置でない）の場合、正当性確認部１０４は、無線通信部１０１を経由して前記接続要求を出した他の無線装置の正当性を確認できなかった（家庭内の無線装置であることが確認できなかった）ことを接続要求応答部１０２へ出力する。すると接続要求応答部１０２は、接続要求を受理できなかったことを示す接続要求受理信号を無線通信部１０１を介して他の無線装置へ出力する。

【００３０】鍵情報管理部１０５は、接続要求応答部１０２が接続要求を受理した場合、暗号化・復号化部１０７で管理していた鍵情報を、第２通信部１０６を介して前記接続要求を出した他の無線装置へ出力する。また、鍵情報管理部１０５は、接続要求応答部１０２が接続要求を受理しなかった場合、暗号化・復号化部１０７で管理していた鍵情報を、第２通信部１０６を介して前記接続要求を出した他の無線装置へは出力しない。

【００３１】暗号化・復号化部１０７は、鍵情報管理部１０５から鍵情報が入力されるとデータ処理部１０８からの送信データを暗号化して無線通信部１０１に出力する。また暗号化・復号化部１０７は無線通信部１０１で受信した暗号化データを復号化してデータ処理部１０８に出力する。しかし、鍵情報管理部１０５から鍵情報が入力されない場合には、暗号化・復号化処理は行わない。

【００３２】このようにして接続要求を出した他の無線装置が正しい無線装置（家庭内の無線装置）の場合通信が行われ、正しくない無線装置（家庭内の無線装置でない）の場合通信が行われない。

【００３３】（接続要求をする無線装置の構成）図１は接続要求に応答する無線装置であったが、次に接続要求



をする側の無線装置について図２を用いて詳細に説明する。

【００３４】図２は、本発明に係る接続要求をする無線装置の構成を説明するためのブロック図である。

【００３５】この無線装置は家庭内に置かれた他の無線装置に対して接続要求を行い、自機が家庭内の無線装置からの接続であるかの確認の問い合わせに適切に応答して接続を確立する。

【００３６】まず、無線装置２００の構成について説明する。

【００３７】図２に示すように、無線装置２００は、他の機器と無線により通信を行う無線通信部２０１、他の無線装置に対して接続要求する接続要求部２０２、自機が他の無線装置と同じ家庭内に存在するか否かの確認に応答する無線装置存在確認応答部２０３、無線通信部２０１を介して他の無線装置からの正当性確認に応答する正当性確認応答部２０４、スクランブルに用いる鍵情報を管理する鍵情報管理部２０５、無線通信部２０１とは別の系（例えば有線）で通信を行う第２通信部２０６、通信するデータを暗号化・復号化する暗号化・復号化部２０７、通信するデータを送受処理するデータ処理部２０８から構成されている。

【００３８】次に、このように構成された無線装置２００の動作について詳細に説明する。

【００３９】接続要求送信部２０２は、無線通信部２０１を介して他の無線装置に対して接続要求を送信する。この接続要求を受けた他の無線装置は、当該他の無線装置内の第２通信部１０６を介して図１で説明した通り存在確認を行うことになる。この存在確認時、無線装置存在確認応答部２０３は、第２通信部２０６を介して他の無線装置と通信を行い存在確認に正しく応答する。この応答後、他の無線装置から第２通信部２０６を介して鍵情報が入力されるので、鍵情報管理部２０５はこの鍵情報を管理する。

【００４０】鍵情報管理部２０５は、管理する鍵情報を正当性確認応答部２０４に出力する。この鍵情報が正当性確認応答部２０４に入力された後、他の無線装置は無線通信部２０１を介して正当性確認を行うことになる。この正当性確認時、正当性確認応答部２０４は、無線通信部２０１を介して他の無線装置と通信を行い、図１で説明した通り正当性の確認を行う。

【００４１】この正当性の確認後、接続要求部２０２は他の無線装置から無線通信部２０１を介して接続要求受理を受け取る。接続要求部２０２が接続要求受理を受け取ると、鍵情報管理部２０５は管理している鍵情報を暗号化・復号化部２０７に出力する。正当性の確認が行われなかった場合には、自機は正しくない無線装置（家庭内の無線装置でない）と接続要求先の他の無線装置に判断されてしまったことになるので通信は行われない。

【００４２】暗号化・復号化部２０７はデータ処理部２

０８から入力された送信データを暗号化して無線通信部２０１を介して他の無線装置に出力する。また暗号化・復号化部２０７は無線通信部２０１で受信した暗号化データを復号化してデータ処理部２０８に出力する。

【００４３】このようにして接続要求を受けた他の無線装置が自機を正しい無線装置（家庭内の無線装置）と判断した場合通信が行われ、正しくない無線装置（家庭内の無線装置でない）合通信が行われない。

【００４４】次に、本発明に係る無線装置が家庭内でどのように接続されるかについて図３を用いて詳細に説明する。

【００４５】図３は、本発明に係る無線装置が家庭内で無線装置の接続を示す図である。この図３では、無線装置Ａは図１で説明した接続要求応答する無線装置、無線装置Ｂおよび無線装置Ｃは図２を用いて説明した接続要求装置であるものとして説明する。

【００４６】無線装置Ｂは無線装置Ａと同一家庭内の装置であり、無線装置Ａと問題なくアクセスする権利がある。無線装置Ｂは無線装置Ａに対して無線経由で接続要求を行う。無線装置Ａは接続要求を受信すると無線装置Ｂに対し鍵情報を、例えば電灯線Ａを経由して送信すると共に、正当性確認のためのメッセージを無線経由で送信する。無線装置Ｂは電灯線Ａより受信した鍵情報を用いて無線経由で受信したメッセージを暗号化して無線装置Ａに返送する。無線装置Ａは無線装置Ｂから届いた暗号化メッセージを電灯線Ａ経由で送付した鍵情報を用いて復号し、送信したメッセージと一致すれば無線装置Ｂは家庭内の装置であると判断して無線通信を許可する。

【００４７】一方、無線装置Ｃは無線装置Ａとは別の家庭内の装置である。この場合、無線装置Ａが無線装置Ｃからの接続要求を許可してしまうと、無線装置Ａの持つ情報を無線装置Ｃが不正に取得できることとなり問題がある。

【００４８】無線装置Ｃが無線装置Ａに接続要求を行った場合、無線装置Ａは無線装置Ｂの場合と同様電灯線Ａを経由して無線装置Ｃに鍵情報を伝送しようとする。しかし無線装置Ｃは隣の家の、電灯線Ａとは別の電灯線Ｂに接続されており、無線装置Ｃは無線装置Ａから鍵情報を受け取ることができない。このため無線装置Ａからの正当性確認に応答することができず、無線装置Ａは不正アクセスと判断して接続要求を破棄する。

【００４９】以上説明したとおり、同一家庭内の装置では接続要求が許可され、同一家庭内に無い装置同士では接続要求が破棄される。

【００５０】なお、図３は電灯線で接続されているものとして説明したが、これに限らず有線で通信ができるものであれば何でも良い。

【００５１】次に、本発明における無線接続の動作手順について図４を用いて詳細に説明する。

【００５２】図４は、本発明における無線接続の動作手順を示す図である。

【００５３】図４において、（手順１）まず無線装置Ｂから無線装置Ａに対し接続要求を送信する。

【００５４】（手順２）次に無線装置Ａから無線装置Ｂに対して電灯線（有線）経由で鍵情報（鍵Ｋ）を送付する。

【００５５】（手順３）無線装置Ａは接続要求装置の正当性を確認する。

【００５６】（手順４）無線装置Ｂは正当性確認に応答する。

【００５７】（手順５）正当性を確認した無線装置Ａは接続要求が受理されたことを無線装置Ｂに通知し、これによりデータ通信が行われる。

【００５８】次に、本発明における無線接続において不正アクセスを排除する場合の動作手順について図５を用いて詳細に説明する。

【００５９】図５は、本発明における無線接続において不正アクセスを排除する場合の動作手順を示す図である。図５において、（手順１）まず無線装置Ｃから無線装置Ａに対し接続要求を送信する。

【００６０】無線装置Ｃからの接続要求を受け取った無線装置Ａは図４の手順２と同様にして無線装置Ｃに対して電灯線Ａを経由して鍵情報（鍵Ｋ）の送付を試みるが、電灯線Ａとは別の電灯線Ｂに接続されているため無線装置Ｃは無線装置Ａから鍵情報を受け取ることができない。このため無線装置Ｃは無線装置Ａからの（手順３）に対して正しい応答（手順４）を返すことが出来ず、（手順５）の接続要求は破棄され、通信することが出来なくなる。

【００６１】次に、本発明における携帯型の無線装置における無線接続の動作手順について図６を用いて詳細に説明する。

【００６２】図６は携帯型の無線装置における接続方法の概略を示す図である。図６において、モバイルオーディオプレーヤ等の携帯型無線装置の場合、通常は電灯線と切り離し持ち歩いて使う。このため接続要求時に電灯線経由で装置を確認することはできない。

【００６３】本発明では携帯型無線装置の場合、図６（ａ）に示す通り一度目については充電用のアダプタを経由して鍵Ｋを送付する。そして図６（ｂ）に示す通り２度目以降については携帯無線装置側はメモリ等に図６（ａ）で保持した鍵情報（鍵Ｋ）を無線装置Ａからの正当性確認には正しく応答することができる。

【００６４】次に、本発明における無線通信手段とは別の通信手段として有線のＩＥＥＥ１３９４を適用した場合について図７および図８を用いて詳細に説明する。

【００６５】図７および図８は無線通信手段とは別の通信手段として有線のＩＥＥＥ１３９４を適用した場合を説明するための図である。図７において、無線装置Ａ，無線装置Ｂ，無線装置Ｃは部屋１に配置されＩＥＥＥ１

３９４を介して接続されており、無線装置Ｘ，無線装置Ｙ，無線装置Ｚは部屋２に配置されＩＥＥＥ１３９４を介して接続されている。但し部屋１のＩＥＥＥ１３９４と部屋２のＩＥＥＥ１３９４とは有線では接続されていない。

【００６６】従来の方式では、無線装置Ａや無線装置Ｘ以外に、無線装置Ｂや無線装置Ｙなど全ての無線装置に鍵情報を設定しなければ、全ての装置間での無線接続はできなかった。

【００６７】本発明によれば、まず無線装置Ａおよび無線装置Ｘは人手による入力やメディア経由等従来の手段を用いて鍵情報の交換を行う。この際無線装置ＡはＩＥＥＥ１３９４接続された無線装置Ｂおよび無線装置Ｃに対してもＩＥＥＥ１３９４経由で鍵情報を伝送する。同様に無線装置Ｘは無線装置Ｙおよび無線装置Ｚに鍵情報を伝送する。

【００６８】これにより無線装置Ａおよび無線装置Ｘだけ設定することにより、ＩＥＥＥ１３９４接続されたこの家庭内全ての装置の無線設定を完了することが出来る。

【００６９】次にこの無線設定後、部屋１と部屋２間で図８に示す通り無線装置を入れ替えた場合の従来の技術と本発明との違いについて説明する。図８は、無線装置Ｂおよび無線装置Ｃが部屋１から部屋２へ移動して有線のＩＥＥＥ１３９４ネットワークに接続され、無線装置Ｘおよび無線装置Ｚが部屋２から部屋１へ移動して有線のＩＥＥＥ１３９４ネットワークに接続された点が図７と比べて変更されている。

【００７０】例えば無線装置Ａと無線装置Ｂとの無線接続について考える。

【００７１】従来の方式では、レイアウト変更前には無線装置Ａと無線装置Ｘとの無線接続設定しか行っておらず、レイアウト変更により別の部屋に切り離されてしまった無線装置Ａと無線装置Ｂに対して新たに設定を行う必要があった。

【００７２】本発明によれば、無線装置Ａと無線装置Ｂは有線ＩＥＥＥ１３９４で接続されていた時に、有線ＩＥＥＥ１３９４経由で無線装置Ａと無線装置Ｙ間で行われた無線接続の設定を無線装置Ｂにも反映させるため、後日有線接続されていない別の部屋に移動した場合でも、無線装置Ａと無線装置Ｂに対して新たに設定することなく無線装置Ａと無線装置Ｂ間で無線通信を行うことができる。

【００７３】このように図８に示す通りレイアウト変更したとしても、図７で接続したときにメモリ等に保持している鍵情報を用いることにより、ＩＥＥＥ１３９４接続時に行った事前の設定により無線通信を開始することができる。

【００７４】次に、本発明における正当性確認の具体的例について図９を用いて詳細に説明する。



【００７５】図９は、接続要求に応答する無線装置と、接続要求する無線装置との間で、装置の正当性を確認する一例を示す図である。ここでは一般的な２パス相手認証による正当性確認の例を示す。認証方法は他にも種々考えられ、本発明はいずれを適用しても良い。正当性の確認は接続要求する無線装置が接続要求に応答する無線装置と同じ鍵情報を保持しているから正当性を判断することができる。同一家庭内の無線装置であれば電灯線等の有線経由で鍵情報を正しく伝送できるので、鍵情報を保有していれば同一家庭内の無線装置と判断することが出来る。

【００７６】次に正当性確認の手順について説明する。接続要求に応答する無線装置Ｂは（手順１）ます乱数Ｒａを発生する。

【００７７】（手順２）次に接続要求に応答する無線装置Ｂこの発生した乱数Ｒａを接続要求する無線装置Ａに送付する。

【００７８】（手順３）接続要求する無線装置Ａは、乱数Ｒａを、メモリ等に保有している鍵情報である鍵Ｋで暗号化する。

【００７９】（手順４）接続要求する無線装置Ａは、接続要求に応答する無線装置Ｂに返送する。

【００８０】（手順５）接続要求に応答する無線装置Ｂは、受信した暗号化鍵Ｋ（Ｒａ）を鍵情報である鍵Ｋで復号化して、もともと保持していた乱数Ｒａと比較する。接続要求する無線装置Ａから送られてきた乱数Ｒａ'が（手順２）で発生した乱数Ｒａと一致すれば、接続要求する装置Ａは鍵情報である鍵Ｋを保持していると判断することができ、同一家庭内の正当なアクセス権をもつ装置と判断することができる。

【００８１】次に、本発明における無線装置の接続要求時に接続要求装置から伝送される装置識別ＩＤについて図１０を用いて詳細に説明する。

【００８２】図１０は、接続要求時に接続要求装置から伝送される装置識別ＩＤの具体例を示す図である。図１０（ａ）に示すエコーネットアドレスは、電灯線を含む家庭内ネットワークの規格であるエコーネットで用いられるアドレスであり、８ｂｉｔのＮｅｔＩＤ（ネットＩＤ）と８ｂｉｔのＮｏｄｅＩＤ（ノードＩＤ）からなる。図１０（ｂ）に示すＩＥＥＥ１３９４アドレスは、ＩＥＥＥ１３９４での通信に用いるアドレスであり、１０ｂｉｔのＢｕｓＩＤ（バスＩＤ）と６ｂｉｔのＮｏｄｅＩＤ（ノードＩＤ）からなる。接続要求する装置から接続要求に応答する無線装置は、このアドレス情報の示す無線装置に鍵情報を伝送する。

【００８３】次に、本発明における接続要求に応答する無線装置Ｂにおける接続要求応答時の動作について図１１を用いて詳細に説明する。

【００８４】図１１は、本発明における接続要求に応答する無線装置Ｂにおける接続要求に応答するときの動作

を示すフローチャートである。図１１において、接続要求に応答する無線装置Ｂは、接続要求する無線装置Ａから接続要求を受信する（ステップ１１０１）。次に、接続要求に応答する無線装置Ｂは、接続要求する無線装置Ａが既に鍵情報を保持しているかを確認する（ステップ１１０２）。

【００８５】接続要求に応答する無線装置Ｂは、ステップ１１０２において、接続要求する無線装置Ａが鍵情報を保持していない場合鍵情報を発生させ（ステップ１１０３）、ステップ１１０４へ進む。また、接続要求に応答する無線装置Ｂは、ステップ１１０２において、接続要求する無線装置Ａが鍵情報を保持している場合にはステップ１１０４へ進む。

【００８６】接続要求に応答する無線装置Ｂは、ステップ１１０４では、鍵情報を有線の通信手段を経由して接続要求する装置に送付する。

【００８７】次に、接続要求に応答する無線装置Ｂは乱数を発生し（ステップ１１０５）、この発生した乱数を無線の通信手段を経由して接続要求する無線装置Ａに送付する（ステップ１１０６）。

【００８８】接続要求する無線装置Ａは、接続要求に応答する無線装置Ｂから暗号化された乱数を無線の通信手段を経由して受信し、これを鍵情報を用いて暗号化した後、接続要求に応答する無線装置Ｂへ送り返す。

【００８９】接続要求に応答する無線装置Ｂは、接続要求する無線装置Ａから暗号化された乱数を受信し、この暗号化された乱数を復号化する（ステップ１１０８）。

【００９０】接続要求に応答する無線装置Ｂは、ステップ１１０８で復号化した乱数と、ステップ１１０５で発生した乱数とが一致するか否かを判定する（ステップ１１０９）。

【００９１】接続要求に応答する無線装置Ｂは、ステップ１１０９の判定の結果、一致する場合には接続要求を受理し（ステップ１１１０）、無線通信を開始する（ステップ１１１１）。反対に、ステップ１１０９の判定の結果、一致しない場合には接続要求を破棄する（ステップ１１１２）。

【００９２】次に、本発明における接続要求する無線装置Ａにおける接続要求時の動作について図１２を用いて詳細に説明する。

【００９３】図１２は、本発明における接続要求する無線装置Ａにおける接続要求するときの動作を示すフローチャートである。図１２において、接続要求する無線装置Ａは、接続要求に応答する無線装置Ｂに対し接続要求を行う（ステップ１２０１）。

【００９４】次に接続要求する無線装置Ａは、接続要求に応答する無線装置Ｂから有線の通信手段を経由して鍵情報を受信する（ステップ１２０２）。

【００９５】次に接続要求する無線装置Ａは、無線手段を経由して乱数を受信する（ステップ１２０３）。



【００９６】次に接続要求する無線装置Ａは、ステップ１２０３で受信した乱数を鍵情報で暗号化する（ステップ１２０４）。

【００９７】次に接続要求する無線装置Ａは、ステップ１２０４で暗号化した鍵情報を接続要求に応答する無線装置Ｂに送付する（ステップ１２０５）。

【００９８】次に接続要求する無線装置Ａは、接続要求に応答する無線装置Ｂで接続が受理された場合、接続要求が受理されたことを示す応答が返るので、これを受信し（ステップ１２０６）、接続要求に応答する無線装置Ｂと無線通信を開始する（ステップ１２０７）。

【００９９】なお、本発明の有線通信装置が電灯線に接続されている場合には、この電灯線は家庭内の別の電灯線に情報を転送するブレーカ装置を含むことにより、電灯線がブレーカをはさんで複数の系統に分割されている場合でも、家庭内の装置を正しく判別することができる。

【０１００】また、装置を識別するための情報は、無線通信のための設定情報とすることにより、接続要求する装置側に無線のための詳細な設定を省略することができる。

【０１０１】

【発明の効果】以上説明したようにこの発明によれば、無線経由で接続要求を行った装置が正当なアクセス権を持つ装置であるかを、同一家庭内のみで終結する第２の通信手段経由で確認しているので、人手による設定を行わずに隣接した家等外部からの不正な接続要求を排除し、同一家庭内の装置のみの安全な無線通信ネットワークを構築することができる。

【図面の簡単な説明】

【図１】本発明に係る接続要求に応答する無線装置の構成を説明するためのブロック図。

【図２】本発明に係る接続要求をする無線装置の構成を説明するためのブロック図。

【図３】本発明に係る無線装置が家庭内で無線装置の接続を示す図。

【図４】本発明における無線接続の動作手順を示す図。

【図５】本発明における無線接続において不正アクセスを排除する場合の動作手順を示す図。

【図６】携帯型の無線装置における接続方法の概略を示す図。

【図７】無線通信手段とは別の通信手段として有線のＩＥＥＥ１３９４を適用した場合を説明するための図。

【図８】無線通信手段とは別の通信手段として有線のＩＥＥＥ１３９４を適用した場合を説明するための図。

【図９】接続要求に応答する無線装置と、接続要求する無線装置との間で、装置の正当性を確認する一例を示す図。

【図１０】接続要求時に接続要求装置から伝送される装置識別ＩＤの具体例を示す図。

15

【図１１】本発明における接続要求に応答する無線装置Ｂにおける接続要求に応答するときの動作を示すフローチャート。

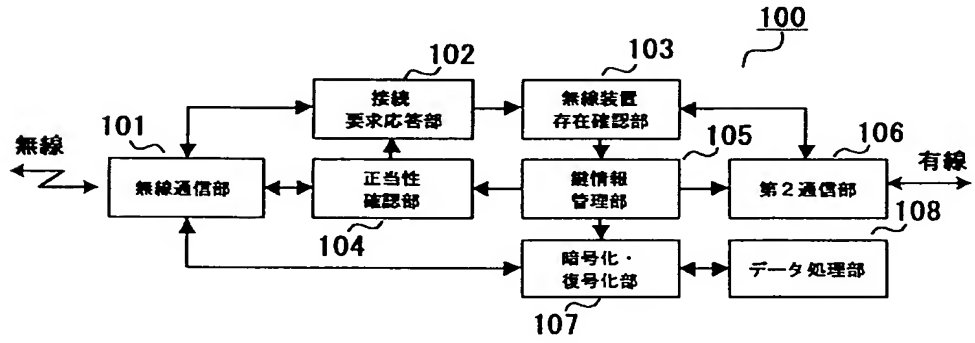
【図１２】本発明における接続要求する無線装置Ａにおける接続要求するときの動作を示すフローチャート。

【符号の説明】

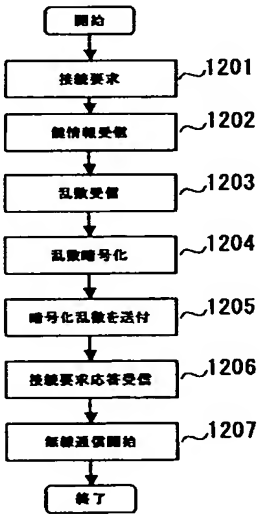
１００、２００…無線装置、１０１、２０１…無線通信部、１０２…接続要求応答部、１０３…無線装置存在確認部、１０４…正当性確認部、１０５、２０５…鍵情報管理部、１０６、２０６…第２通信部、１０７、２０７…暗号化・復号化部、１０８、２０８…データ処理部、２０２…接続要求送信部、２０３…無線装置存在確認応答部、２０４…正当性確認応答部。

16

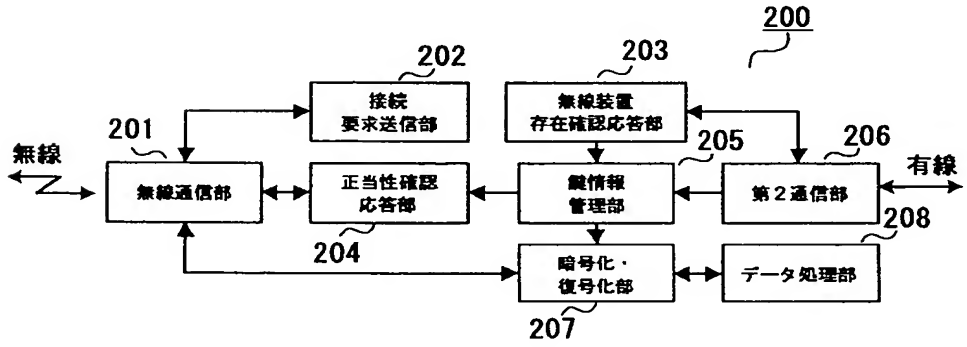
【図１】



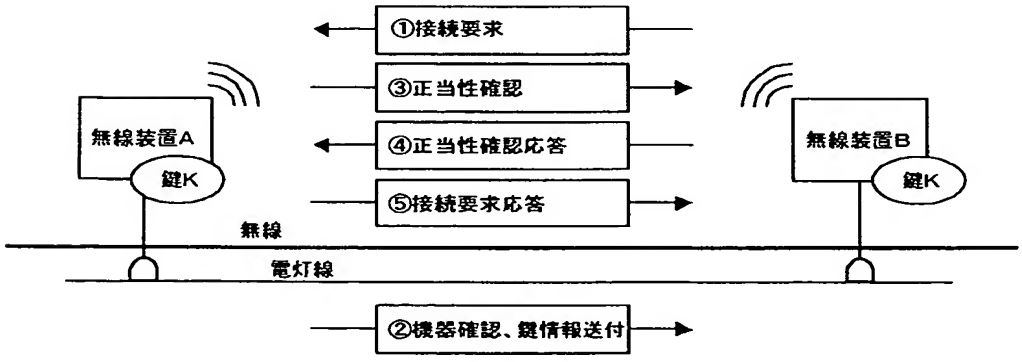

【図１２】



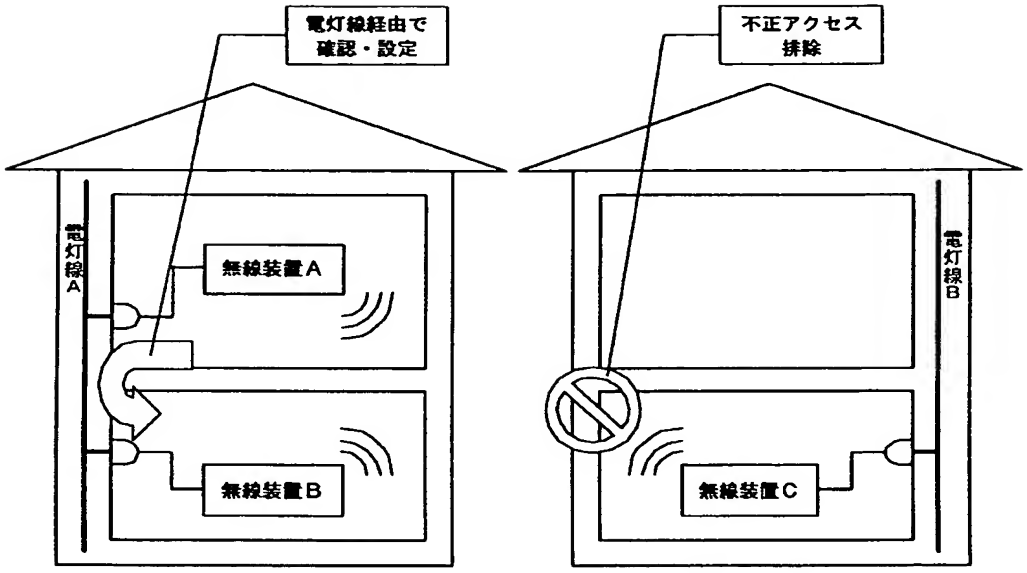

【図２】



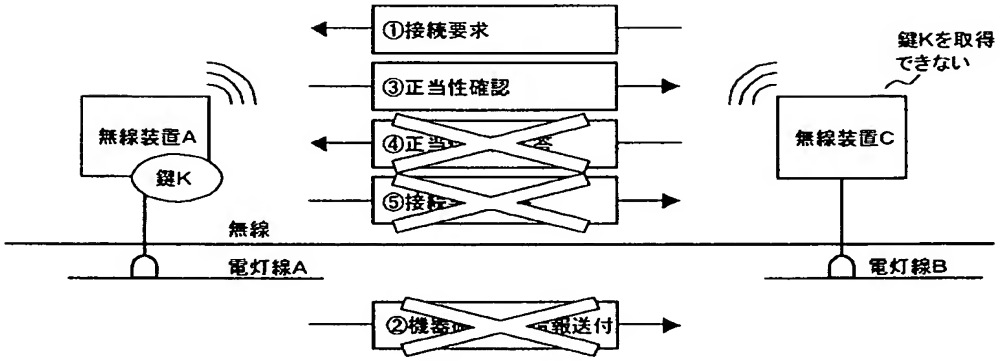

【図４】



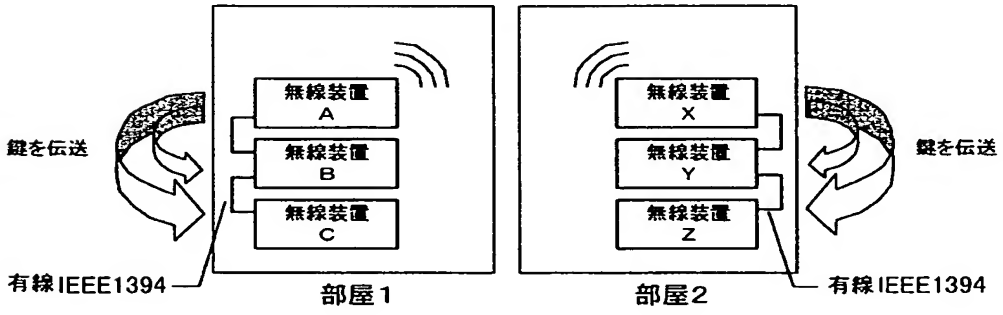
【図３】


電灯線経由で
確認・設定
不正アクセス
排除
電灯線A
無線装置A
無線装置B
無線装置C
電灯線B

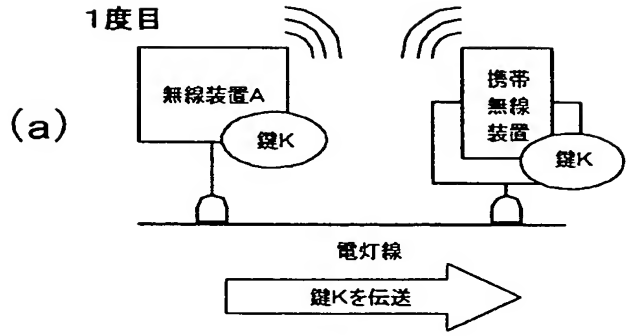
【図５】


①接続要求
③正当性確認
④正当
⑤接続
②機器
報送付
鍵Kを取得
できない
無線装置A
鍵K
無線装置C
無線
電灯線A
電灯線B

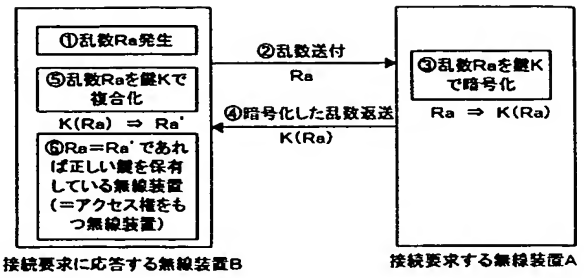
【図７】


無線装置
A
無線装置
B
無線装置
C
無線装置
X
無線装置
Y
無線装置
Z
鍵を伝送
鍵を伝送
有線IEEE1394
有線IEEE1394
部屋1
部屋2

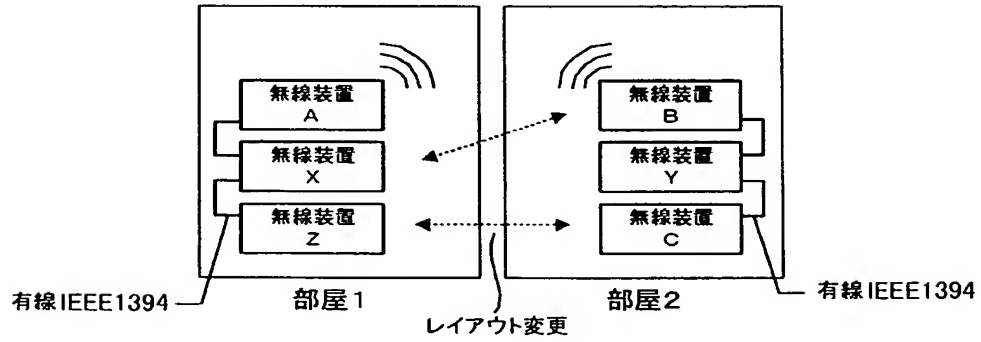
【図６】


1度目
(a)
無線装置A
鍵K
携帯
無線
装置
鍵K
電灯線
鍵Kを伝送
2度目以降
(b)
無線装置A
鍵K
携帯
無線
装置
鍵K
電灯線

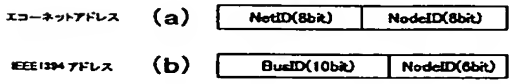
【図９】


①乱数Ra発生
⑤乱数Raを鍵Kで複合化
K(Ra) ⇒ Ra'
⑥Ra=Ra'であれば正しい鍵を保有している無線装置（＝アクセス権をもつ無線装置）
接続要求に応答する無線装置B
②乱数送付
Ra
④暗号化した乱数返送
K(Ra)
③乱数Raを鍵Kで暗号化
Ra ⇒ K(Ra)
接続要求する無線装置A

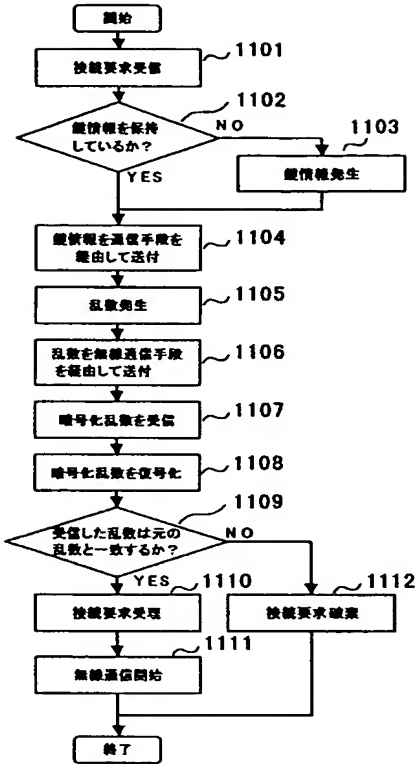
【図８】


無線装置
A
無線装置
X
無線装置
Z
無線装置
B
無線装置
Y
無線装置
C
有線IEEE1394
部屋１
部屋２
有線IEEE1394
レイアウト変更

【図１０】


エコーネットアドレス
(a)
NetID(8bit)
NodeID(8bit)
IEEE1394 アドレス
(b)
BusID(10bit)
NodeID(6bit)

【図１１】




---

フロントページの続き

| (51) Int. Cl.[7] | 識別記号 | F I | テーマコード（参考） |
|---|---|---|---|
| H04L 12/40 | | H04L 9/00 | 601E<br>651 |

(72)発明者　茶木　宏之
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内

Ｆターム(参考)　5J104 AA15 AA16 EA04 EA16 EA24 NA02
5K032 AA08 BA01 DA02 DA20
5K033 AA08 BA01 CB01 DA02 DA13 DA17 DB23
5K046 AA03 PS43